FortiClient (Android) - User Guide

VERSION 5.2.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

August 22, 2015

FortiClient (Android) 5.2.6 User Guide

04-526-288761-20150822

TABLE OF CONTENTS

Change Log

Date	Change Description
2014-06-13	Initial release.
2014-07-08	Updated for 5.2.1.
2014-08-01	Updated for 5.2.2.
2014-08-20	Updated for 5.2.3.
2014-10-09	Updated for 5.2.4.
2015-08-22	Updated for 5.2.6.

Introduction

FortiClient (Android) 5.2 has been redesigned to include IPsec VPN, SSL VPN, Web Security, and Endpoint Control.

FortiClient (Android) 5.2 features

The following table lists and describes features supported in FortiClient (Android) 5.2.

Feature	Description
IPsec VPN	• Configure IPsec VPN connections. • IKE main mode and aggressive mode support. • Client X.509 certificates and pre-shared key support. • Enable always up and auto connect options. • Disable auto start.
SSL VPN	• Configure tunnel mode SSL VPN connections. • Client and server X.509 certificates support. • Enable always up and auto connect options. • Disable auto start.
Web Security	• Allow or deny web browsing based on FortiGuard groups and categories. • Monitor web browsing violations • Client Web Filtering when On-Net.
Endpoint Control	• Configure and deploy a FortiOS FortiClient Profile to registered FortiClient (Android) devices. • Provision a Web Category Filtering profile and VPN connections. • Policy enforcement.

Download FortiClient (Android) 5.2.6

You can download the FortiClient (Android) 5.2.6 application from the Google play application or at the following link, https://play.google.com/store.

Product Integration and Support

FortiClient (Android) 5.2.6 support

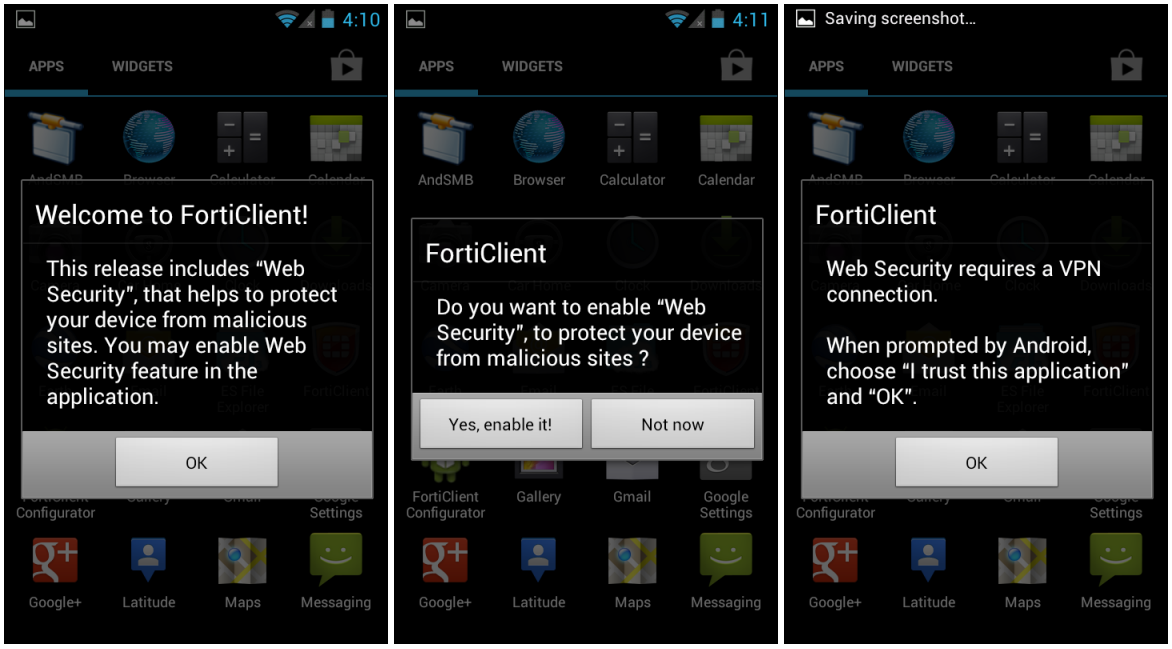
The following table lists FortiClient (Android) 5.2.6 product integration and support information.

Android operating systems	• 4.1 Jelly Bean (API level 16) • 4.2 Jelly Bean (API level 17) • 4.3 Jelly Bean (API level 18) • 4.4.3 KitKat (API level 19) • 4.4.4 KitKat (API level 20) • 5.0.1 Lollipop (API level 21) • 5.1.1 Lollipop (API level 22)
FortiOS	• 5.0.5 and later • 5.2.0 and later
FortiToken Mobile	• 2.0.3 and later For more information, see the FortiToken Mobile User Guide for Android.

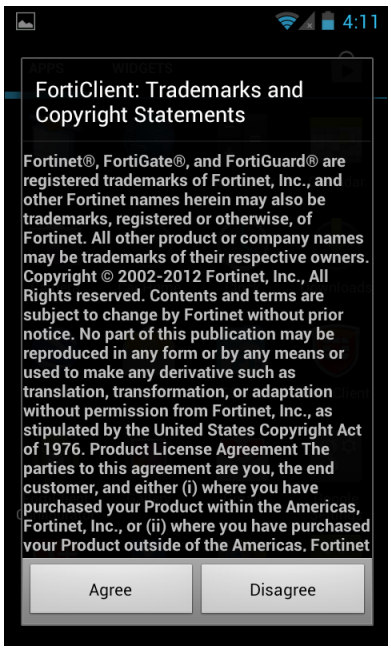
Open the Application

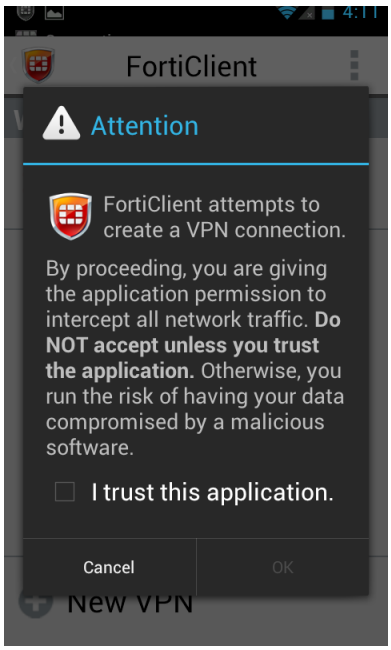
When FortiClient (Android) 5.2 is installed and run for the first time, read the *Trademarks and Copyright Statement* and select the *Agree* button. FortiClient (Android) includes a Web Security feature to help protect your device from malicious sites. When opening FortiClient, you will be prompted to enable the Web Security feature. An *Attention* pop-up dialog window will be displayed noting the FortiClient attempts to create a VPN connection. Read the statement, select the *I trust this application* checkbox, and select *OK*. After that, FortiClient (Android) will automatically start when Android OS starts.

Opening pages



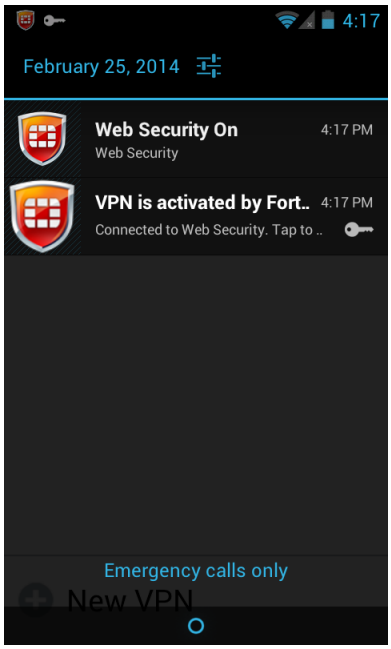
Trademarks and VPN message





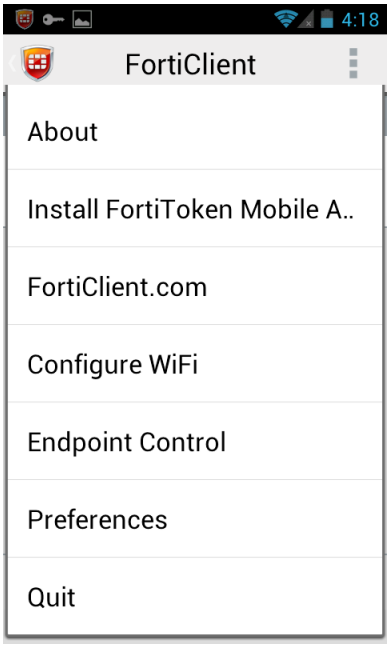
FortiClient (Android) 5.2 allows you to launch the application from the notification bar.

Launch from notification bar



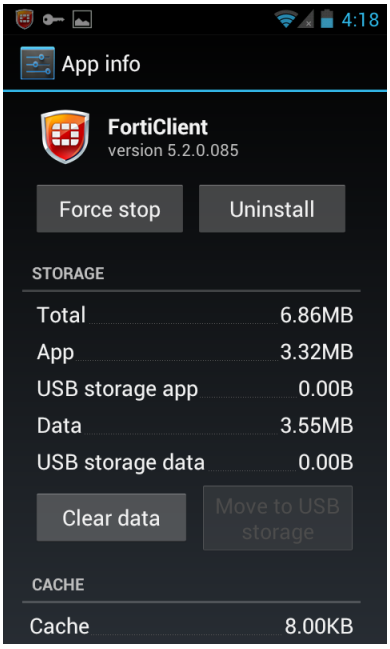
You can quit the app from the menu page.

Quit from app menu



When the Web Security feature is enabled, FortiClient (Android) runs in the background to provide the service. To quit the application, go to the Android OS Settings page, select *Apps*, select *FortiClient*, and select *Force stop*. On this page you can also clear data and uninstall FortiClient (Android).

Apps page



Web Security

FortiClient (Android) 5.2 includes a web security feature to allow you to control web browsing on your Android device. You can select to allow or deny sites based on the FortiGuard site rating. The following table lists the web security groups and categories.

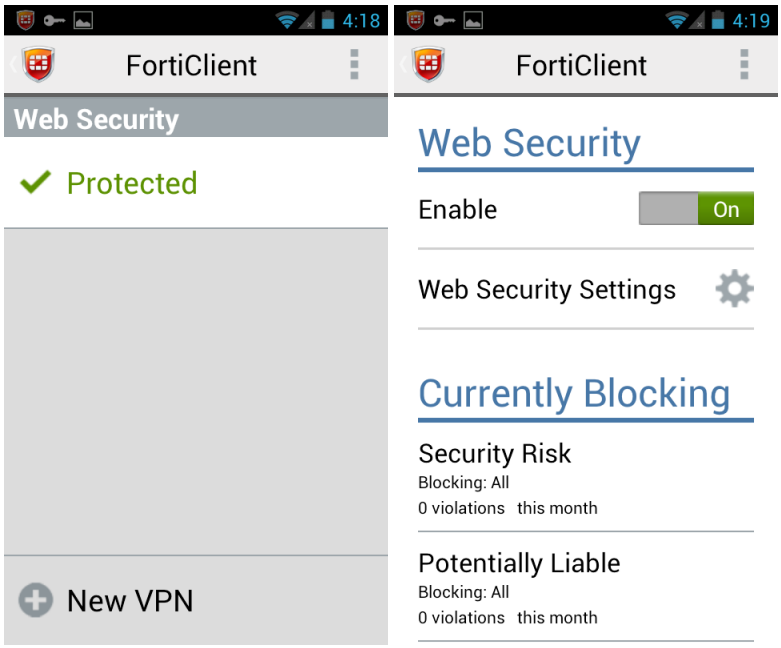
Groups	Categories
Security Risk	Malicious Websites, Phishing, Spam URLs
Potentially Liable	Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Explicit Violence, Extremist Groups, Proxy Avoidance, Plagiarism, Child Abuse
Adult/Mature Content	Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Nudity and Risque, Pornography, Dating, Weapons (Sales), Marijuana, Sex Education, Alcohol, Tobacco, Lingerie and Swimsuit, Sports Hunting and War Games
Bandwidth Consuming	Freeware and Software Downloads, File Sharing and Storage, Streaming Media and Download, Peer-to-peer File Sharing, Internet Radio and TV, Internet Telephony
General Interest - Business	Finance and Banking, Search Engines and Portals, General Organizations, Business, Information and Computer Security, Government and Legal Organizations, Information Technology, Armed Forces, Web Hosting, Secure Websites, Web-based Applications
General Interest - Personal	Advertising, Brokerage and Trading, Games, Web-based Email, Entertainment, Arts and Culture, Education, Health and Wellness, Job Search, Medicine, News and Media, Social Networking, Political Organizations, Reference, Global Religion, Shopping and Auction, Society and Lifestyles, Sports, Travel, Personal Vehicles, Dynamic Content, Meaningless Content, Folklore, Web Chat, Instant Messaging, Newsgroups and Message Boards, Digital Postcards, Child Education, Real Estate, Restaurant and Dining, Personal Websites and Blogs, Content Servers, Domain Parking, Personal Privacy
Unrated	Unrated

The Web Security module is only available in the full FortiClient (Android) app.

For more information on FortiGuard groups and categories, see http://www.fortiguard.com/static/webfiltering.html.

Web security status

The web security status will display *Protected* or *Unprotected*. When this feature is enabled, select *Protected* to view the blocked categories and the number of violations this month.



Enable and disable web security

To enable web security, select *Unprotected*, then toggle the *Enable* switch to *On*. To disable web security, toggle the *Enable* switch to *Off*.

When FortiClient is managed by FortiGate Endpoint Control, the user cannot enable or disable web security.

Web security settings

To change web security settings, select Web Security Settings. There are seven top level groups with various categories. When you select a top level group a drop-down menu will appear. You can select to *Allow All*, *Deny All*, or select to allow or deny each category independently.

When FortiClient is managed by FortiGate Endpoint Control, the web security setting is deployed from FortiGate, and the user cannot change it.

When browsing to a website which falls into a category which is denied, you will receive a web page blocked page.

SSL VPN

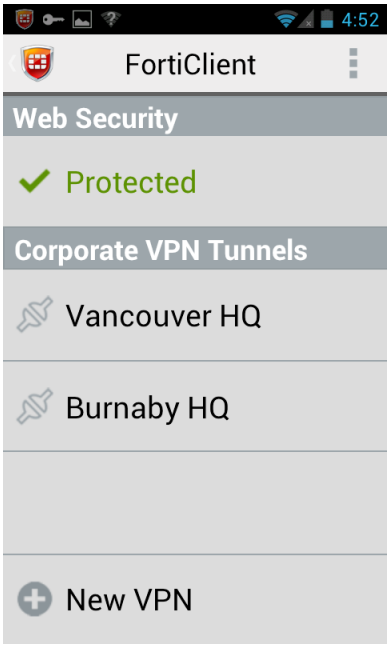
FortiClient (Android) 5.2 supports tunnel mode SSL VPN connections. You can either configure the SSL VPN in the FortiClient user interface or provision SSL VPN connections in the FortiGate FortiClient Profile. Provisioned SSL VPN configurations are pushed to your Android device upon successful registration with the FortiGate device for Endpoint Control. You can configure X.509 certificates, CA server certificates, and check server certificates. You can also configure always up and auto connect for the VPN connection.

Create an SSL VPN connection

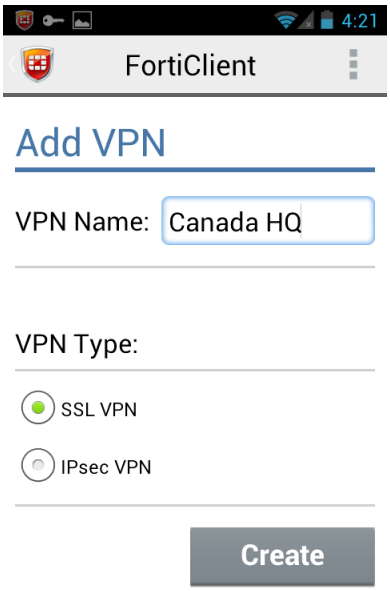
To create a new SSL VPN connection in the FortiClient (Android) user interface follow the steps listed below.

To create a new SSL VPN connection:

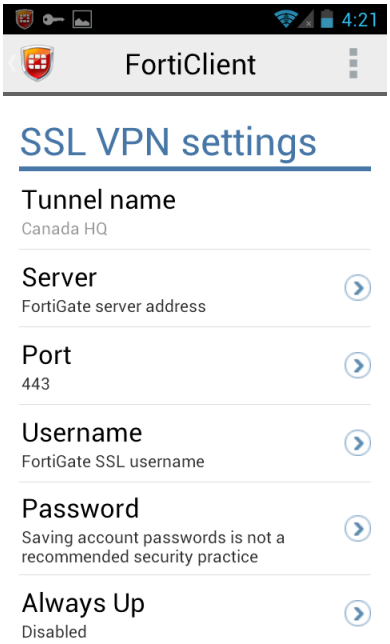
1. Select *New VPN* from the toolbar in the bottom of the page.



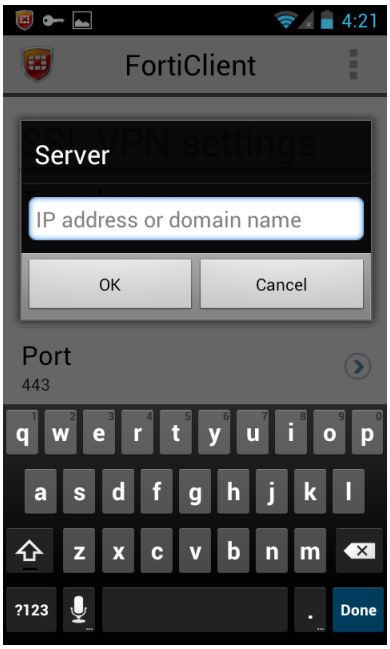
2. Enter a name for the new VPN connection, select *SSL VPN* under *VPN Type*, and select *Create*.



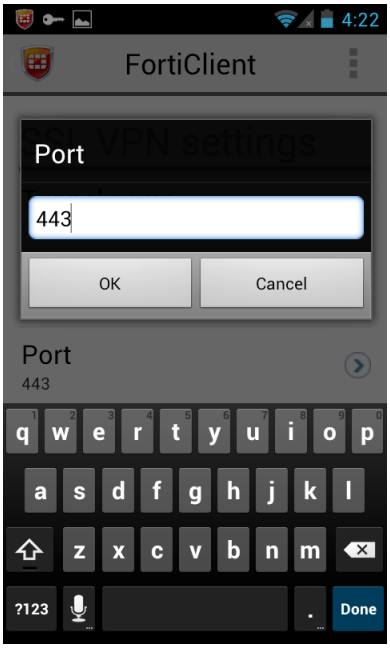
The SSL VPN settings page is displayed.



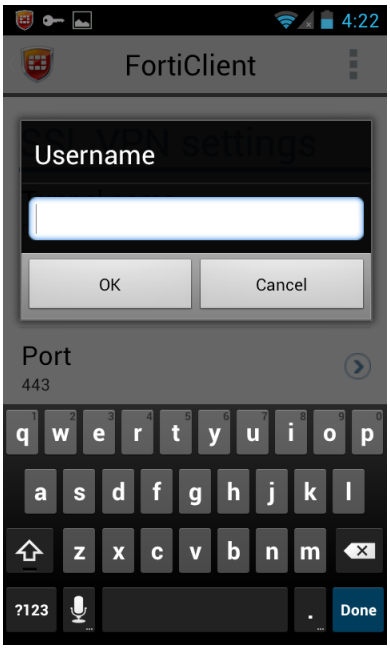
3. Select *Server*, enter the server IP address or domain name, and select *OK*.



4. Select *Port*, enter the port number, and select *OK*. The default port is 443.

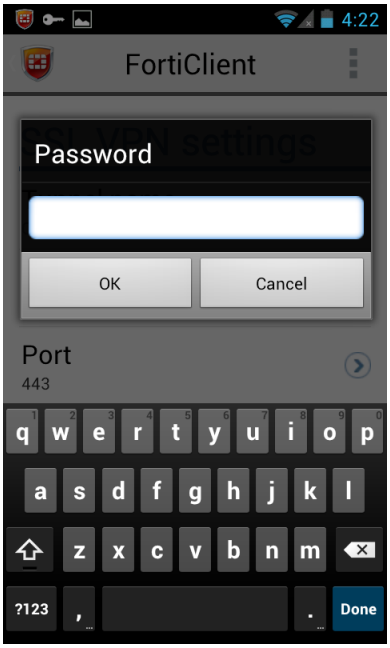


5. Select *Username*, enter a user name, and select *OK*.

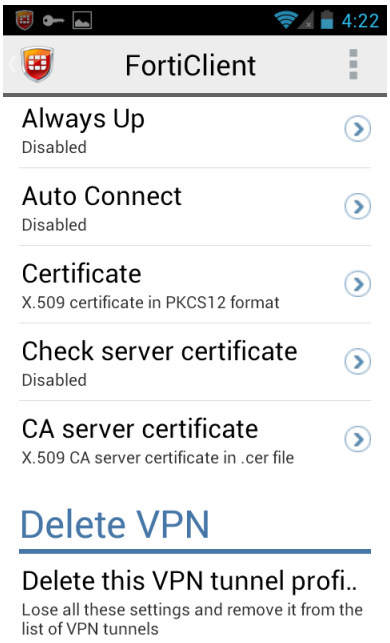


6. Select *Password*, enter a password, and select *OK*. There is no maximum value for the password length. The password can consist of alpha, numeric and special characters.

⚠	The username and password configured on the client must match the username and password configured on the FortiGate. Contact your network administrator for the correct setting.



7. You can select to enable *Always Up*, *Auto Connect*, and *Check server certificate* in the *SSL VPN settings* page.

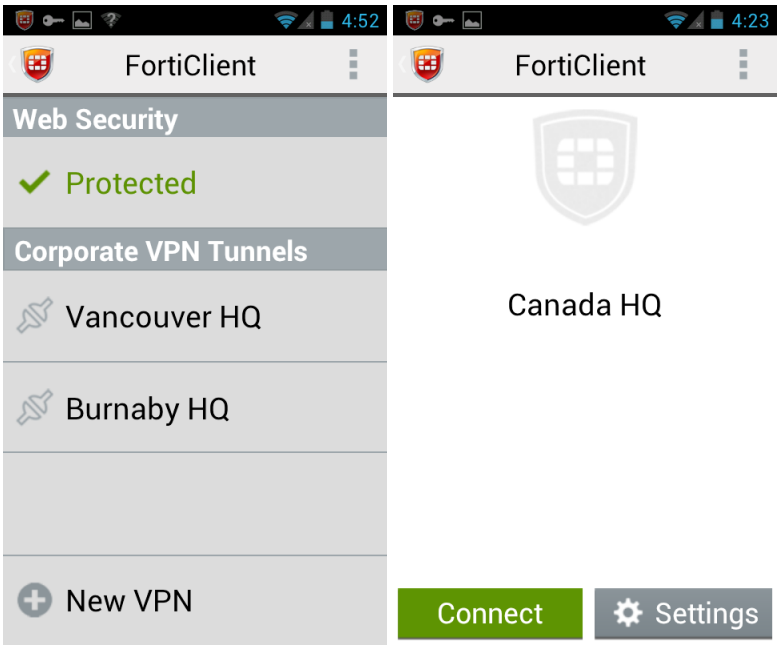


Connect to the VPN

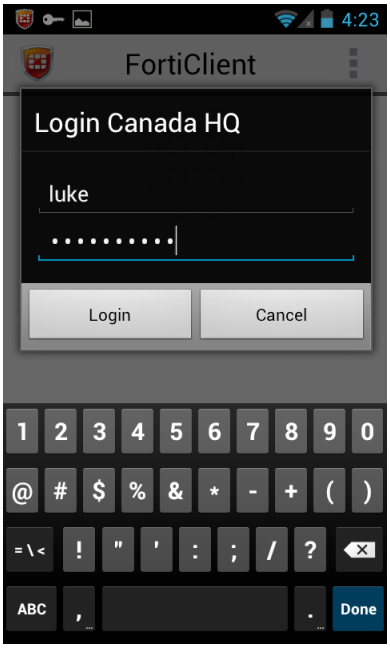
SSL VPN tunnel mode uses X.509 Certificates (PKCS12 format) for authentication. Certificate settings need to be configured if authentication requires the client certificate, otherwise leave the certificate settings as their default value.

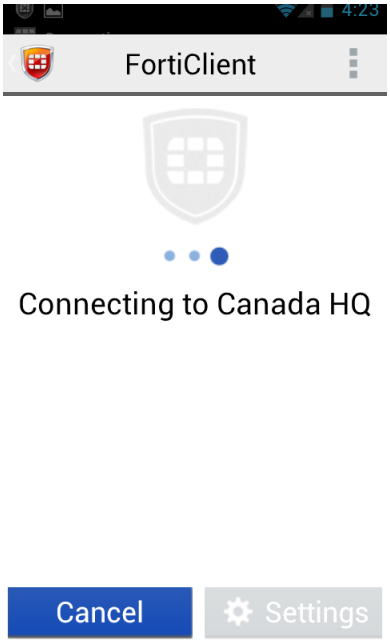
To connect to the SSL VPN:

1. Select an available VPN and then select *Connect*.

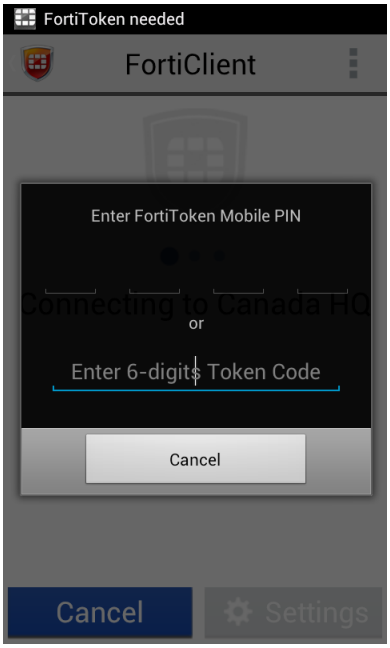


2. Enter your username and password and then select *Login*.

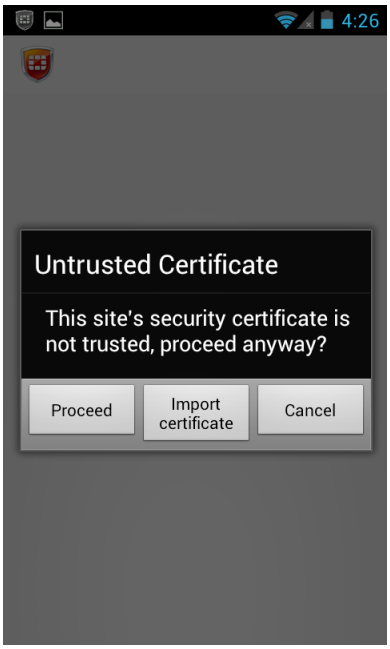




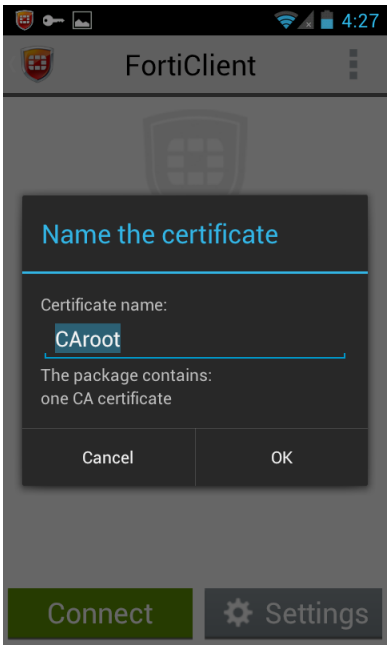
If the SSL VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token.



3. You will receive an *Untrusted Certificate* message dialog box warning message, and you will have the option to *Proceed*, *Cancel*, or *Import certificate*.



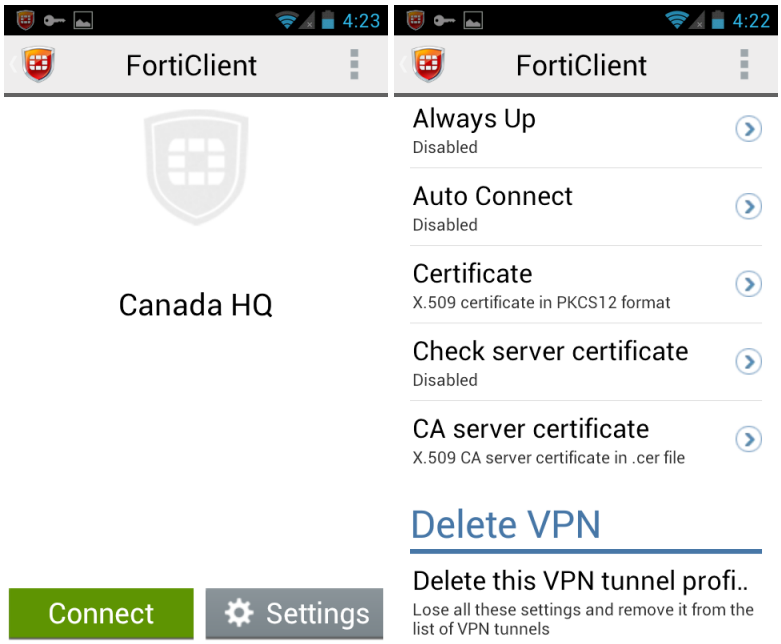
4. Select *Import certificate*, browse for the certificate file, edit the name (if required).



5. Select *OK* to load and install the certificate. The certificate is now installed on the device. Use the device back button to return to the connection screen.
6. Select an available VPN to connect.

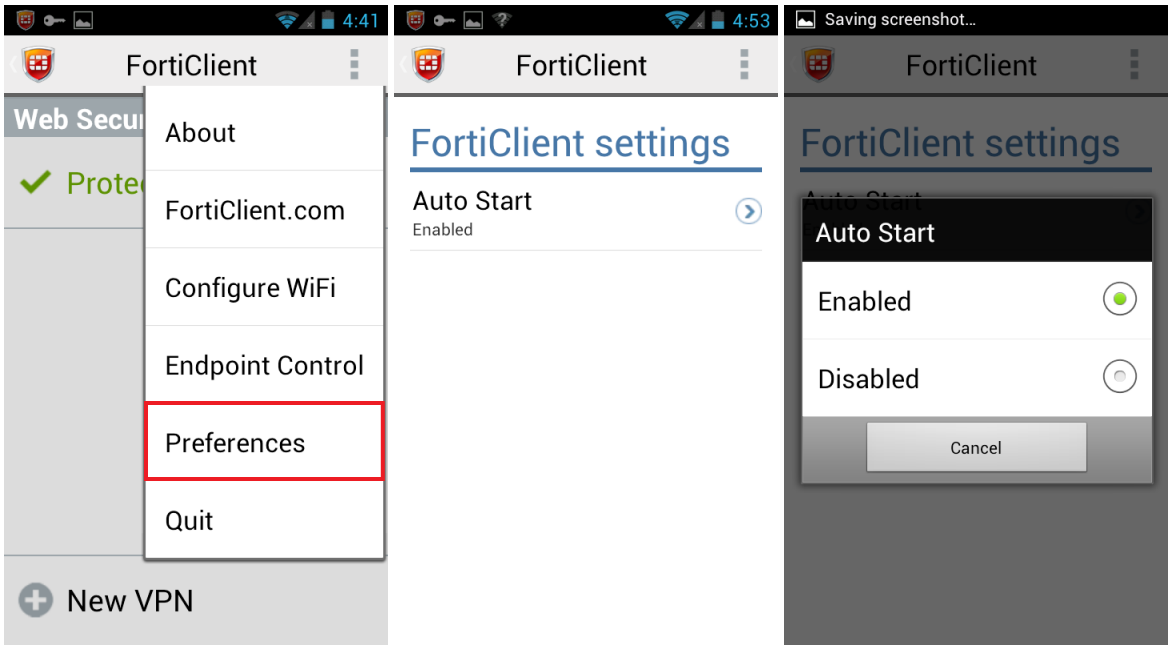
Edit SSL VPN settings or delete a SSL VPN configuration

To edit SSL VPN settings or delete an existing SSL VPN configuration, select the SSL VPN, and select the *Settings* button.



Auto start

In previous FortiClient (Android) versions, VPN auto start was enabled by default. In FortiClient (Android) 5.2 you can select to disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Preferences* in the drop-down menu. In the FortiClient settings page select *Auto Start* and select *Enabled* or *Disabled*.


4:41
FortiClient
About
FortiClient.com
Configure WiFi
Endpoint Control
Preferences
Quit
New VPN
4:53
FortiClient
FortiClient settings
Auto Start
Enabled
Saving screenshot...
FortiClient
FortiClient settings
Auto Start
Enabled
Disabled
Cancel

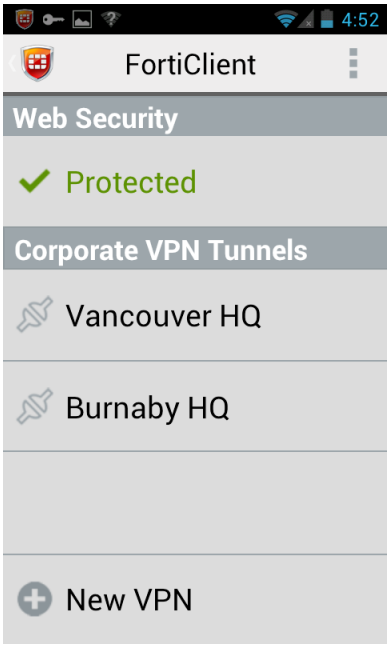
IPsec VPN

FortiClient (Android) 5.2 supports IPsec VPN connections. You can either configure the IPsec VPN in the FortiClient user interface or provision IPsec VPN connections in the FortiGate FortiClient Profile. Provisioned IPsec VPN configurations are pushed to your Android device upon successful registration with the FortiGate device for Endpoint Control. You can configure server settings, phase 1, phase 2, and XAuth settings.

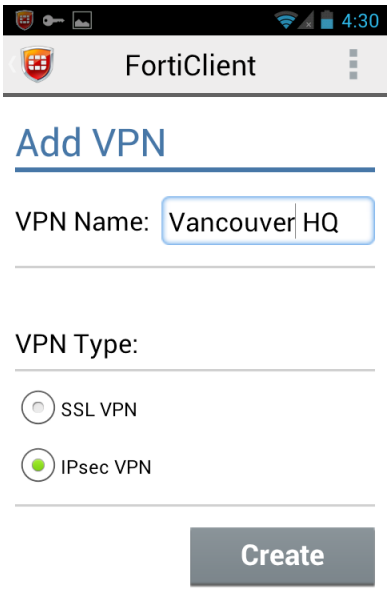
Create an IPsec VPN connection

Create a new IPsec VPN connection:

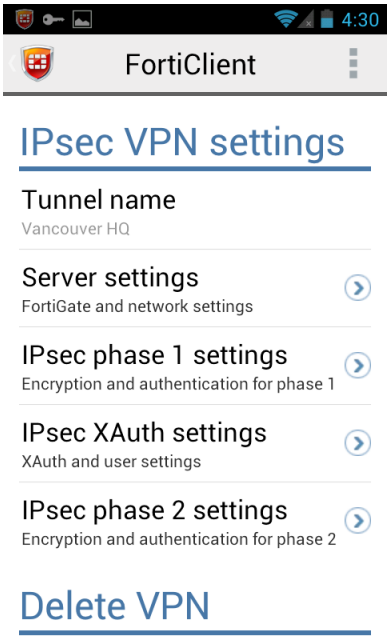
1. Select *New VPN* from the toolbar in the bottom of the page.



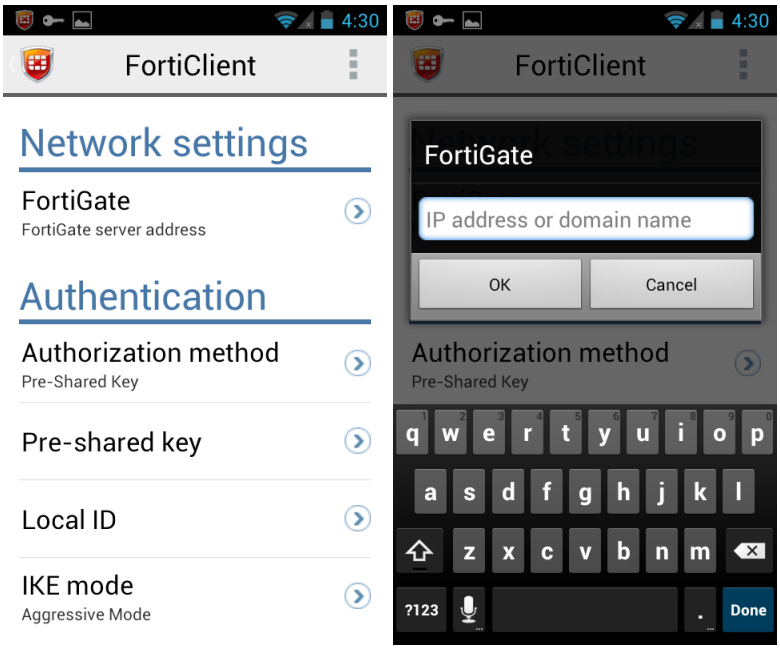
2. Enter a name for the new VPN connection, select *IPsec VPN* under *VPN Type*, and select *Create*.



The IPsec VPN settings page is displayed.



3. Select *Server settings*, under *Network settings*, select *FortiGate*, enter the server IP address or domain name, and select *OK*.

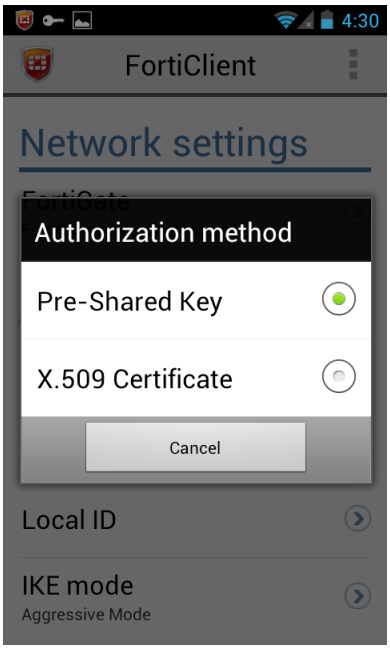


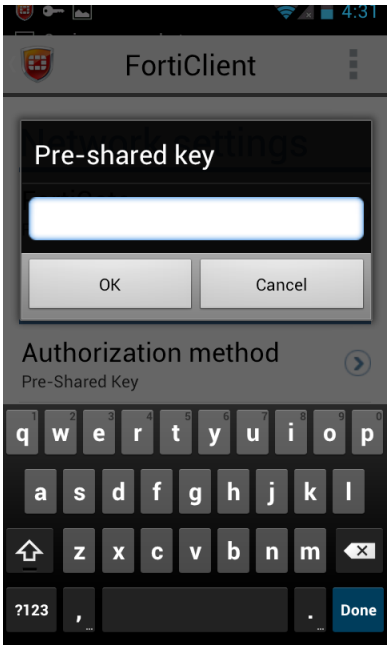
4. Under *Authentication*, select *Authorization method*, and select either *Pre-Shared Key* or *X.509 Certificate*.
5. For pre-shared key, select *Pre-shared Key* to enter the pre-shared key value.

   The simplest way to authenticate with the FortiGate unit is by means of a pre-shared key. This is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth).

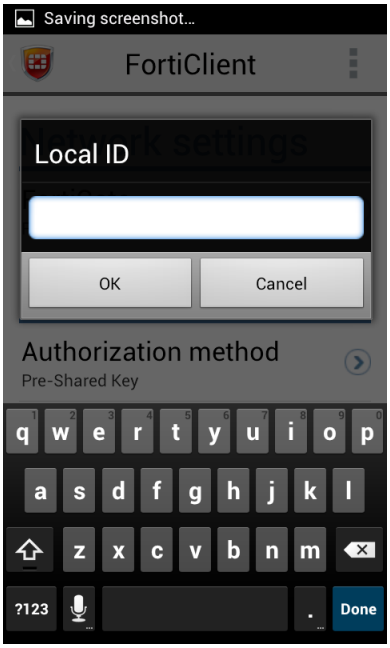
   The pre-shared key must contain at least 6 characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.

⚠	The pre-shared key configured on the client must match the pre-shared configured on the FortiGate. Contact your network administrator for the correct setting.





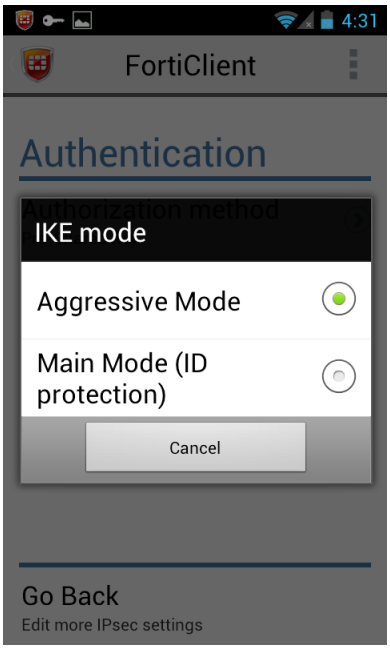
Select *Local ID*, enter the local ID, and select *OK*.



6. For X.509 certificate select *Certificate* and then browse for the certificate file on your device.
   To authenticate with the FortiGate unit using digital certificates, you must have the required certificates installed on the Android device (peer) and the FortiGate unit (server).

⚠	Contact your network administrator for the correct X.509 certificate file.

7. Select *IKE mode*, and select *Aggressive Mode* or *Main Mode (ID protection)*.



In *Aggressive Mode*, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

In *Main Mode*, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.

The *IKE Mode* selected on the client must match the mode selected on the server. Contact your network administrator for the correct setting.

8. Select *Go Back* to return to the *IPsec VPN settings* page.
9. Select *IPsec phase 1 settings* to view or edit the phase 1 proposal encryption and authentication settings. You can choose to use the default settings.

   Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

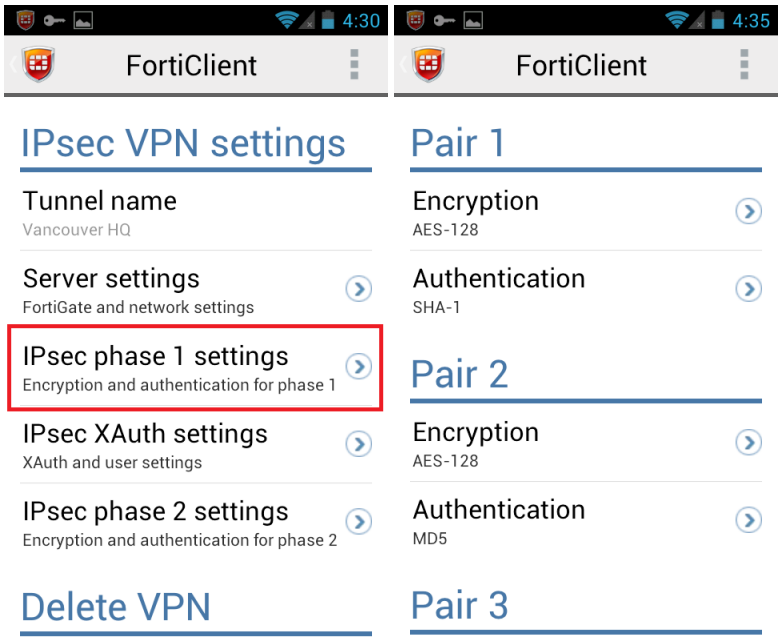
   - DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
   - 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
   - AES128: A 128-bit block algorithm that uses a 128-bit key.

   You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

   - MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
   - SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

   Select one or more Diffie-Hellman (DH) groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.

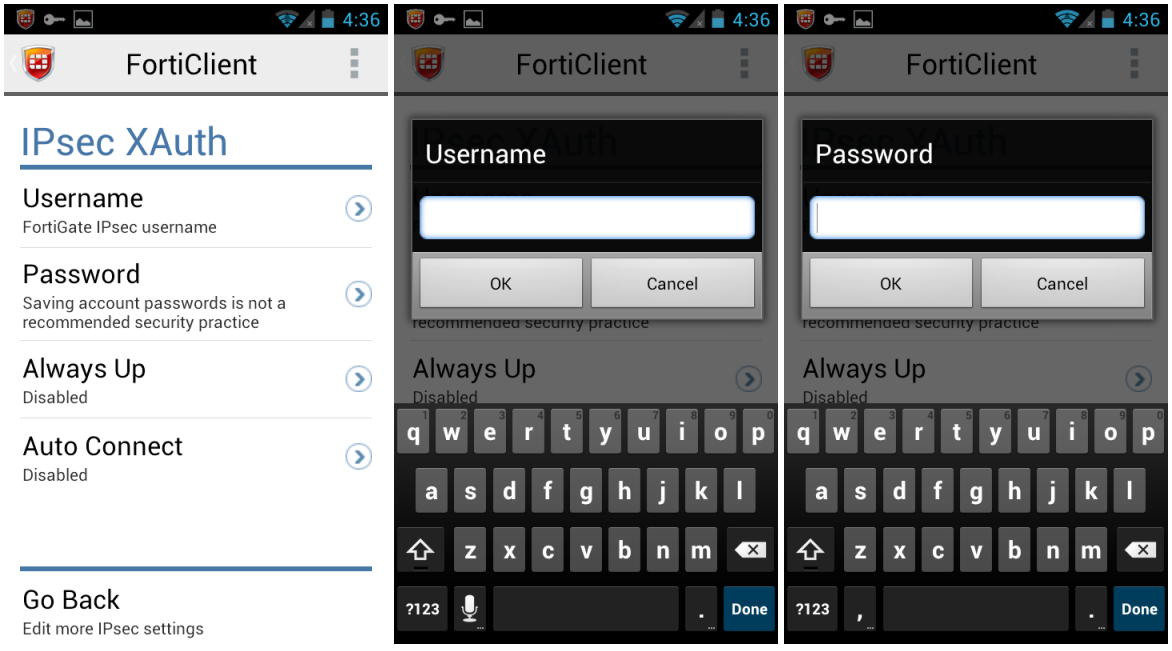
Contact your network administrator for the correct phase 1 encryption and authentication algorithms, and DH group.



10. Select *Go Back* to return to the *IPsec VPN settings* page.
11. Select *IPsec XAuth settings* to view or edit the XAuth and user settings. XAuth is enabled by default. Select *Username* to enter the FortiGate IPsec username. Select *Password* to enter the password value. To use XAuth, you must first configure the user's credentials on your FortiGate, and external RADIUS or LDAP server.

    Extended authentication (XAuth) increases security by requiring the remote dialup client user to authenticate in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS and LDAP to authenticate dialup clients.

    You can select to enable *Always Up*, *Auto Connect*, and *Check server certificate* in the *IPsec XAuth* page.



12. Select *Go Back* to return to the *IPsec VPN settings* page.

13. Select *IPsec phase 2 settings* to view or edit the phase 2 encryption and authentication settings. You can choose to use the default settings.

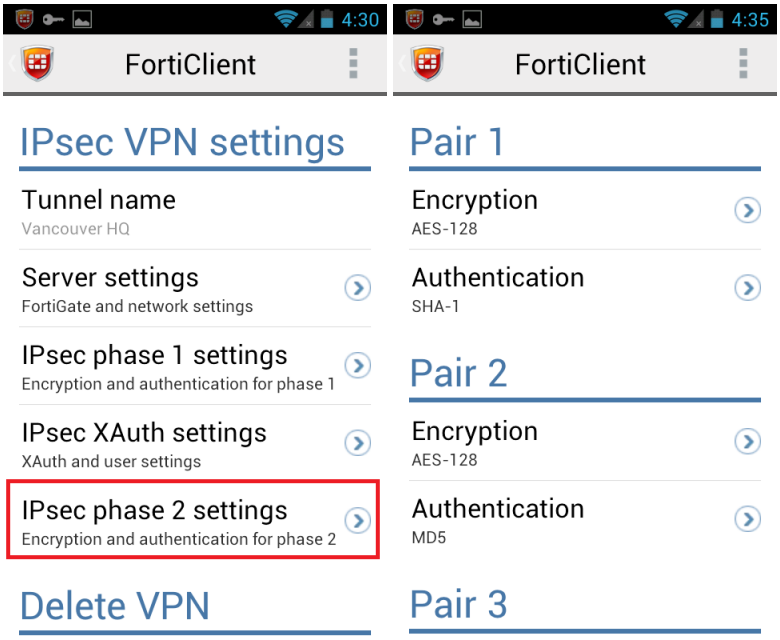
    Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

    - DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
    - 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
    - AES128: A 128-bit block algorithm that uses a 128-bit key.

    You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

    - MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
    - SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

    Select one or more Diffie-Hellman groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.



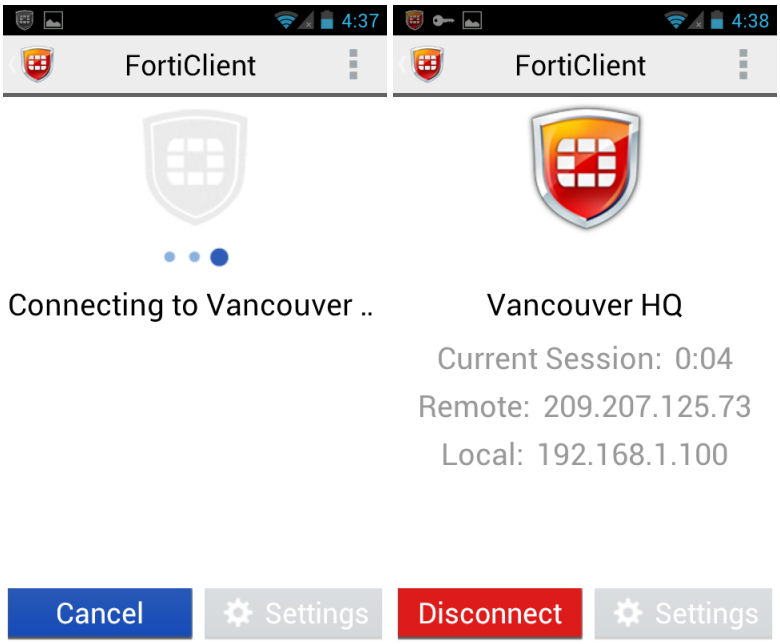
Contact your network administrator for the correct phase 2 encryption and authentication algorithms, and DH group.

14. Select *Go Back* to return to the *IPsec VPN settings* page.

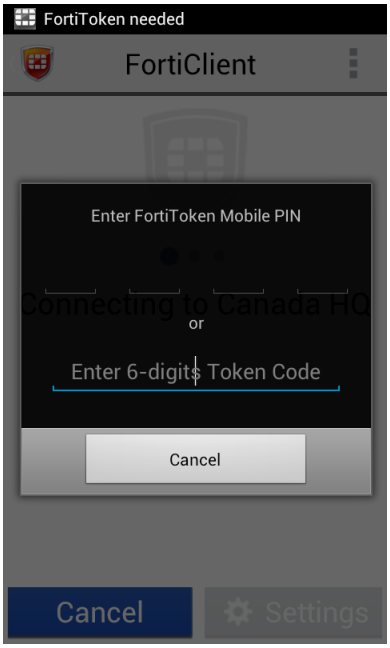
Connect to an IPsec VPN

Connect to an IPsec VPN:

1. Select an available IPsec VPN connection.
2. Enter the username and password, and select *Connect*.

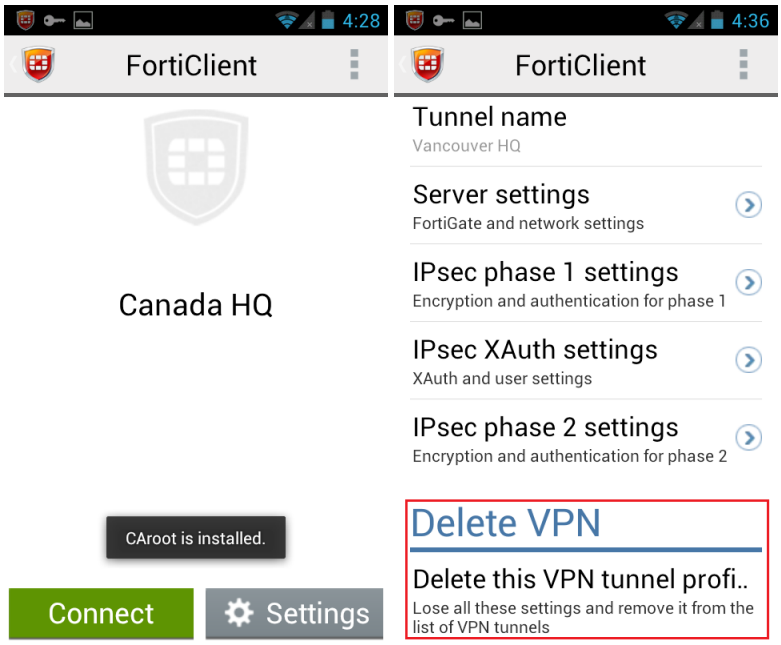


If the IPsec VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token code.



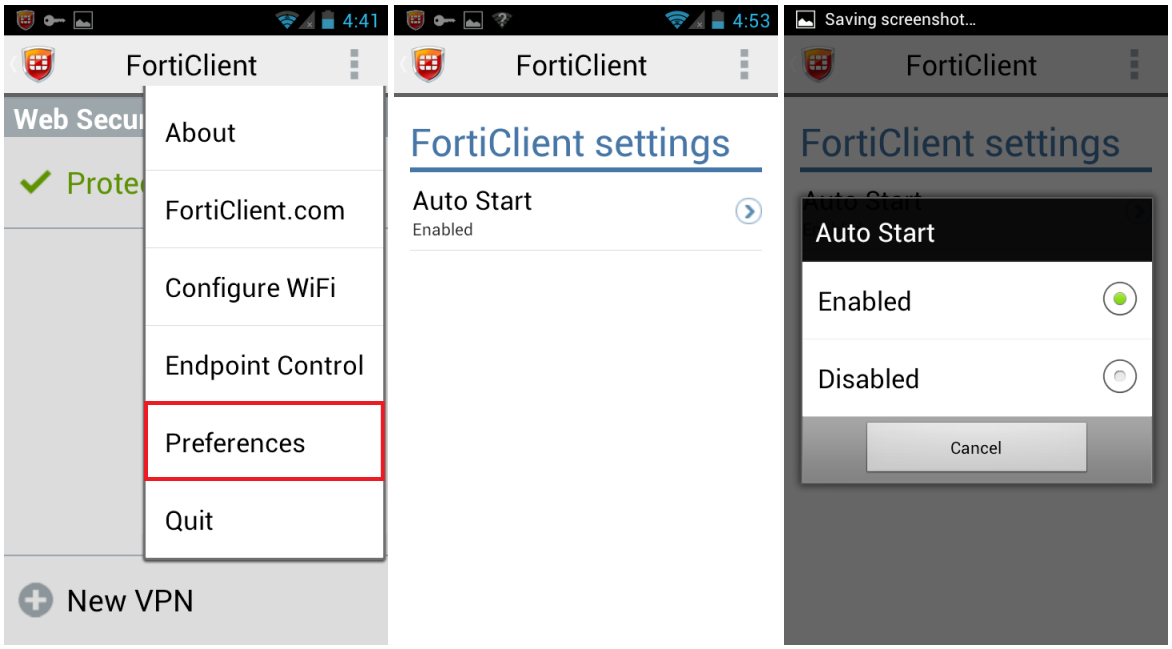
Edit VPN settings or delete a VPN configuration

To edit IPsec VPN settings or delete an existing IPsec VPN configuration, select the IPsec VPN, and select the *Settings* button.



Auto start

In previous FortiClient (Android) versions, VPN auto start was enabled by default. In FortiClient (Android) 5.2 you can select to disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Preferences* in the drop-down menu. In the FortiClient settings page select *Auto Start* and select *Enabled* or *Disabled*.



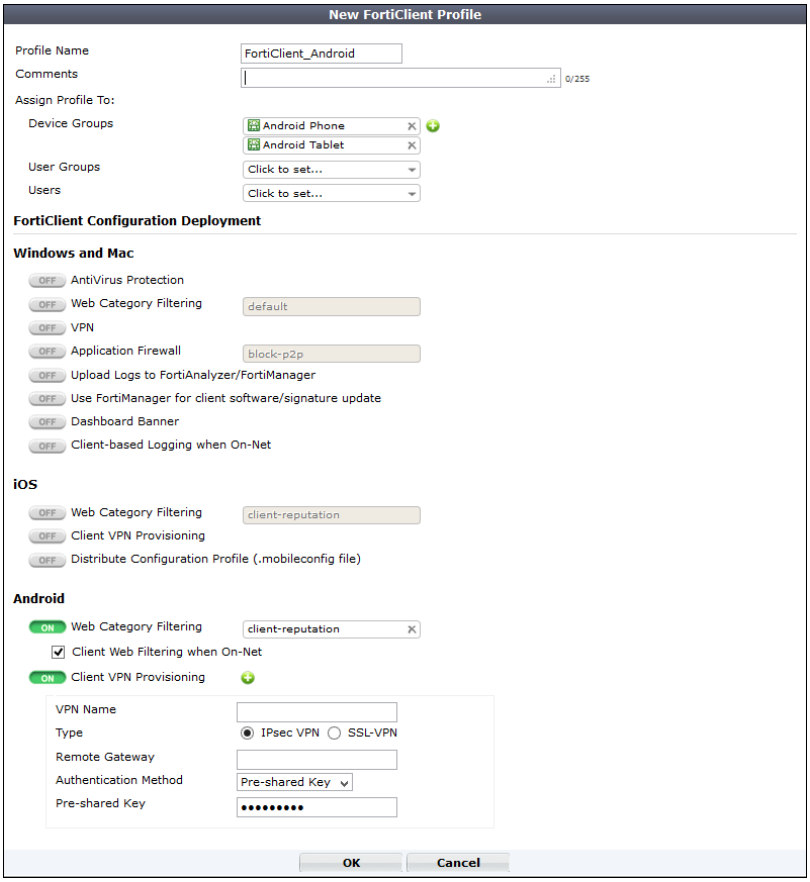
Endpoint Control

FortiClient (Android) 5.2 allows you to register to a FortiGate device and receive a FortiClient profile for endpoint control.

FortiGate FortiClient Profile

Configure the FortiClient Profile:

1. On your FortiGate device, go to *User & Device* > *FortiClient Profiles*.
2. Select *Create New* from the toolbar. The *New FortiClient Profile* page opens.



3. In the *Android* section of the page, configure the following settings:

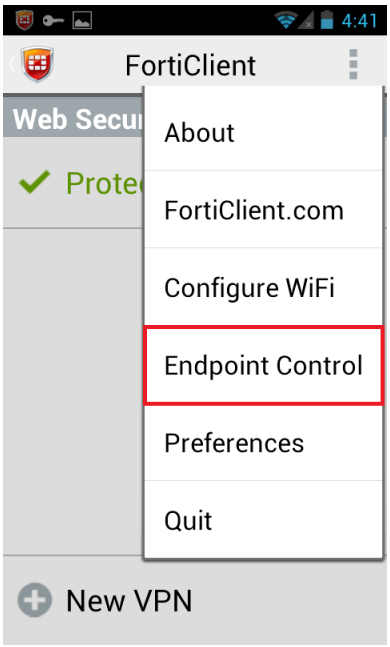
Web Category Filtering		Toggle the button to enable or disable Web Category Filtering. Select the Web Filter profile from the drop-down list. Note: FortiClient (Android) only supports FortiGuard Categories settings in the *Web Filter Profile*. Only *Allow* and *Block* actions are supported. All other settings will be ignored by FortiClient (Android).
	Client Web Filtering when On-Net	Select the checkbox to disable Web Category Filtering when on-net. FortiClient (Android) determines the client to be on-net when the registered FortiGate serial number matches one of the serial numbers it gets from the FortiGate DHCP server. Otherwise it is off-net.
Client VPN Provisioning		Toggle the button to enable or disable client VPN provisioning. Select the add icon to add multiple VPN configurations.
	VPN Name	Enter a name for the VPN connection.
	Type	Select either IPsec VPN or SSL VPN.
	Remote Gateway	Enter the remote gateway.
	Authentication Method	Configure authentication settings. The options available are dependent on the type of VPN selected.

4. Select *OK* to save the settings.

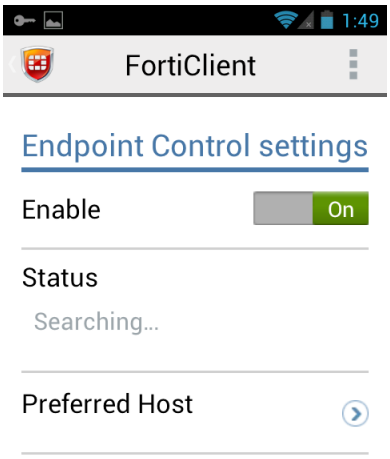
Register to FortiGate

Register to the FortiGate:

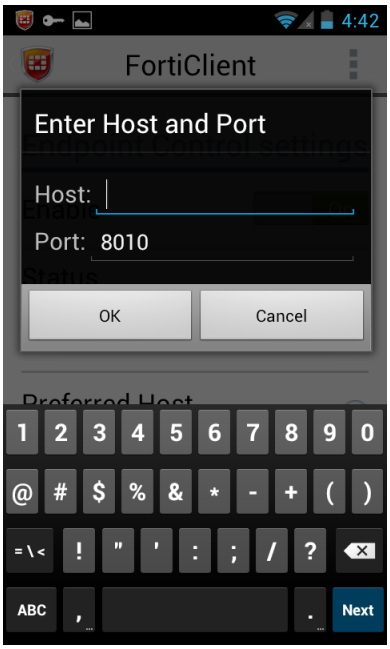
1. On your Android device, open the FortiClient application.
2. Select the menu icon in the toolbar and select *Endpoint Control*.



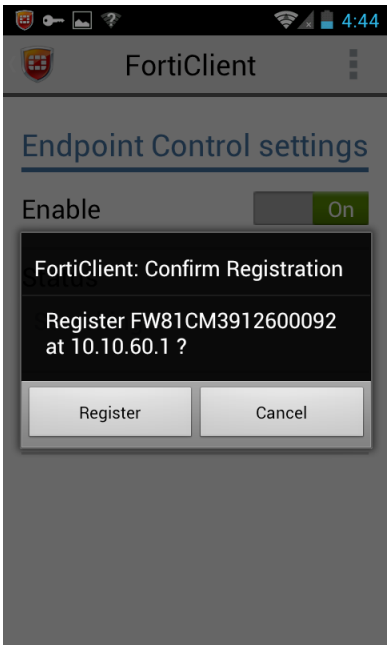
3. In *Endpoint Control settings* toggle the *Enable* switch to *On*.

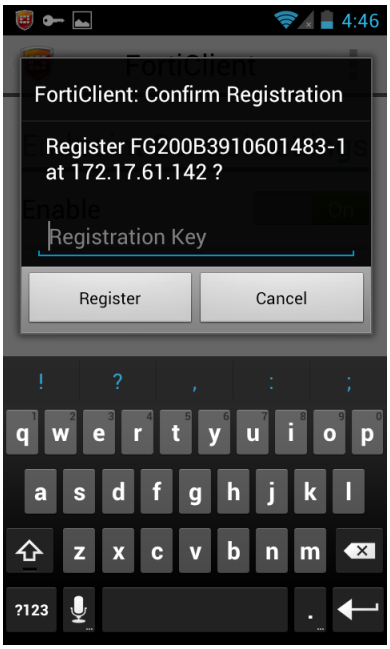


4. FortiClient will search for available FortiGate devices. Alternatively, you can select *Preferred Host* and enter the FortiGate host IP and port number.

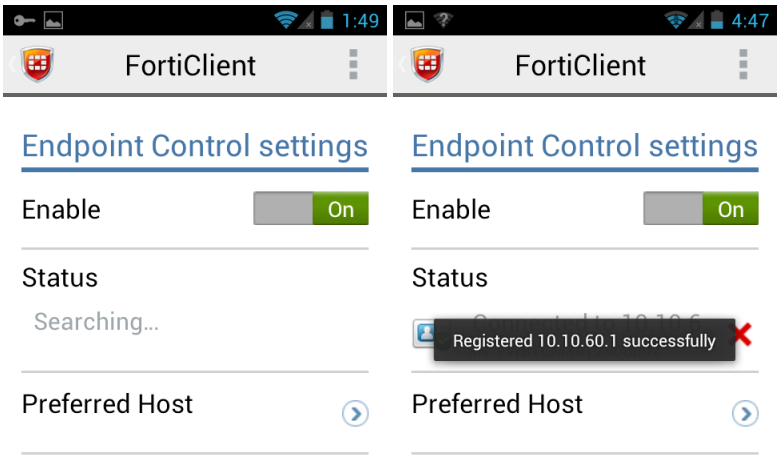


5. When a FortiGate is discovered you will receive a confirm registration dialog box with the FortiGate serial number and IP address. Depending on the FortiGate configuration, you may be required to enter a FortiClient registration key.

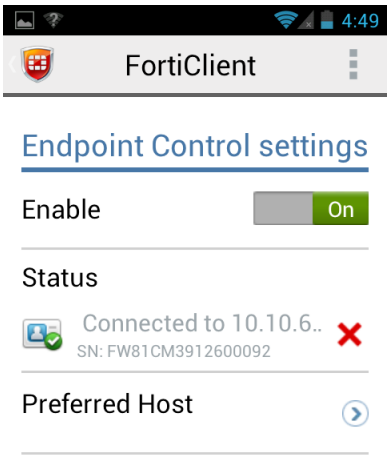




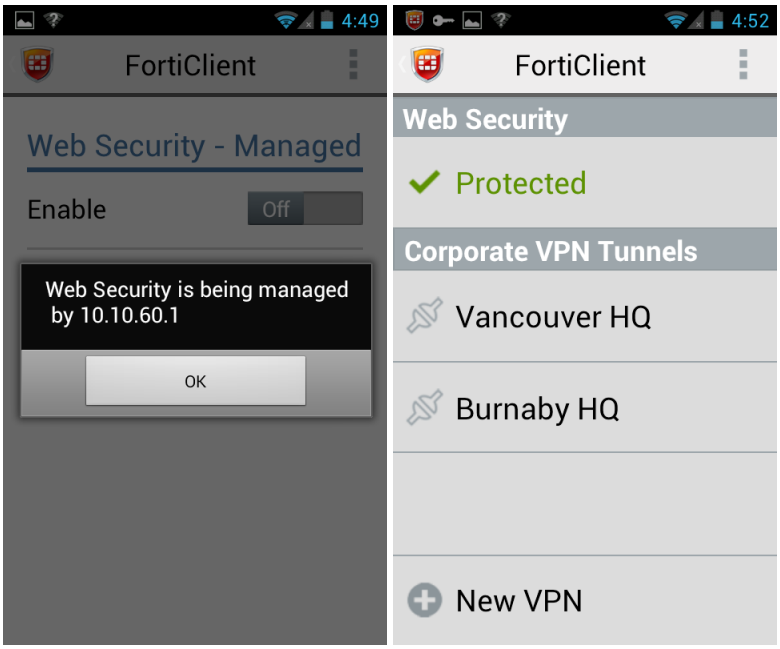
6. Select the *Register* button to continue. You will receive a confirmation dialog box when registration is complete.



7. The *Endpoint Control settings* page will display a connected status.



8. Upon successful registration with FortiGate, FortiClient (Android) will receive the FortiClient Profile. The following image provides an example of a registered FortiClient (Android) with Web Category Filtering and provisioned VPN connections.

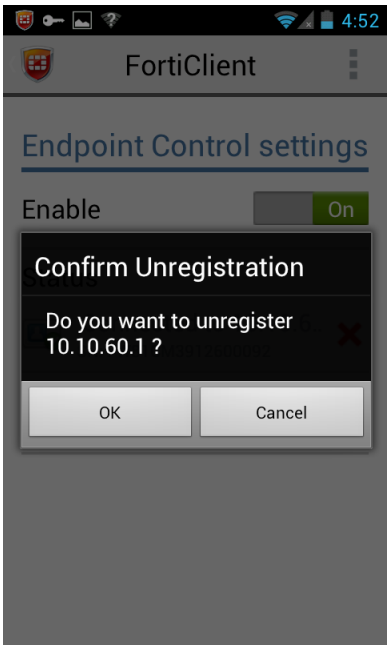


If FortiClient (Android) is registered to FortiGate, it will auto start when the phone is turned on and bring up the GUI.

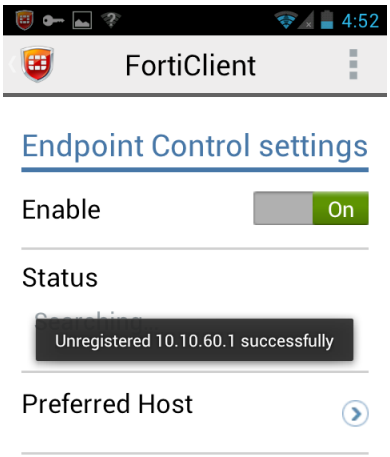
Unregister from FortiGate

To unregister from FortiGate:

1. To unregister from FortiGate, in *Endpoint Control* settings page, in the *Status* section, select the close icon.
2. You will receive a confirmation dialog box.



3. Select *OK* to unregister from the FortiGate. You receive a confirmation dialog box advising that you are unregistered from the FortiGate.



4. Toggle the *Endpoint Control Enable* switch to *Off*.